HP StorageWorks

4000/6000/8000 Enterprise Virtual Array release notes

Part number: 5697-5334
First edition: June, 2005

Legal and notice information

4000/6000/8000 Enterprise Virtual Array release notes

Release notes contents

The *HP StorageWorks 4000/6000/8000 Enterprise Virtual Array release notes* cover the following topics:

- Features and enhancements
- Enterprise Virtual Array overview
- Supported components
- Operating constraints
- Avoiding problem situations
- Documentation updates

NOTE:

Much of the information included here is not documented elsewhere, so it is recommended that you read this information thoroughly before installing and operating the EVA 4000/6000/8000.

The information in this document was the current at the time of publishing. To ensure you have the most current information, check the following web sites for a newer edition:

http://www.hp.com/go/eva4000

http://www.hp.com/go/eva6000

http://www.hp.com/go/eva8000

Intended audience

This document is intended to assist those involved in the installation and operation of the HP StorageWorks 4000/6000/8000 Enterprise Virtual Array and the following associated software:

- HP StorageWorks XCS virtual controller software 5.020 media kit for dual HSV210/200 controllers
- HP StorageWorks Business Copy EVA 3.0
- HP StorageWorks Continuous Access EVA 2.1
- HP StorageWorks Replication Solutions Manager (RSM) 1.1

Additional Enterprise Virtual Array information

Additional information for the EVA 4000/6000/8000 and associated software is listed in Table 1.

Table 1 Additional information

Information	Location
General EVA 4000/6000/8000	http://h18006.www1.hp.com/storage/arraysystems.html
Enterprise Virtual Array product support	http://h18000.www1.hp.com/products/storageworks/enterprise
HP StorageWorks Command View EVA	http://h18006.www1.hp.com/products/storage/software/cmdvieweva/index.html
HP StorageWorks Business Copy EVA	http://h18006.www1.hp.com/products/storage/software/bizcopyeva/index.html
HP StorageWorks Continuous Access EVA	http://h18006.www1.hp.com/products/storage/software/conaccesseva/index.html
Downloadable software and drivers for storage products	http://welcome.hp.com/country/us/eng/support.html
Storage Management Appliance updates	http://h18000.www1.hp.com/products/sanworks/managementappliance
License key redemption	http://h18000.www1.hp.com/products/software/softwarekeys/index.html

Features and enhancements

HP StorageWorks 4000/6000/8000 Enterprise Virtual Array provides the features and enhancements listed below. These elements are detailed in the sections that follow.

- Ease of management
- Data availability
- Performance
- Scalability
- Operating system support
- Fault management and diagnostics
- EVA remote support tools
- Customer self repair

Ease of management

Easy-to-use storage management tools:

- Software tools that allow you to manage larger SAN configurations with more servers and more storage solutions
- HP-supplied disk drives conform to the enclosure-initiated Enclosure Services Interface (ESI)
- State-of-the-art controller software
- Completely integrated configurations with a single part number, plus disk drives and XCS

Data availability

- Redundant hardware design and value–added software eliminate single points of failure from server to storage in clustered or single server configurations with multiple pathing.
- Full support for local and remote data replication using optional HP StorageWorks Business Copy EVA and HP StorageWorks Continuous Access EVA applications.
- Dual– and multi–node cluster support provided for host–level fault tolerance and high system availability.

Performance

Outstanding self-tuning performance includes:

- Virtualization technology—Vraid, enables data to be distributed from 8 to 240 disks to increase disk spindle count far beyond traditional RAID sets. This virtualization method also optimizes storage for the best performance of a specific configuration and application. Enterprise Virtual Array eliminates tedious management functions to provide the best performance possible.
- Both online high-performance and Fibre Attached Technology Adapted (FATA) disk drives.
- State-of-the-art controller software that improves performance, increases capacity, and allows for easy dynamic storage expansion.

Scalability

Support for the following disk capacities:

- 300-GB FC disk drives
- 250-GB FATA disk drives
- 146-GB FC disk drives
- 72-GB FC disk drives
- High-density packaging and support of more disks per controller pair

The EVA8000 offers:

- Up to 200 TB of addressable disk data. With 300–GB drives, a single 42U rack has 50.4–TB of capacity. Using an expansion rack, this can be increased to 72–TB of capacity.
- A maximum of 240 disk drives
- Support for 1024 LUNs

The EVA6000 offers:

- Up to 70 TB of addressable disk data (33.6–TB rack capacity using 300–GB drives) in a 42U rack.
- A maximum of 112 disk drives
- Support for 1024 LUNs

The EVA4000 offers:

- Up to 70 TB of addressable disk data (16.8–TB rack capacity using 300–GB drives) in a 42U rack.
- A maximum of 56 disk drives
- Support for 1024 LUNs

Operating system support

- HP–UX
- Microsoft Windows 2003
- Microsoft windows 2000
- HP Open VMS
- Sun Solaris
- IBM–AIX
- Linux

NOTE:

Direct connect configurations are supported on Microsoft Windows only.

Fault management and diagnostics

WEBES must be installed to ensure proper customer alerts for their EVA products. WEBES can be used as part of the HP ISEE remote service offering. Or, for those customers who do not wish to have remote support, it can be configured to send a local notification (email) to a customer-identified account only. The e-mail option is also available to the customer when ISEE is used.

WEBES is a powerful service tool that provides real-time diagnosis of hardware events ranging from single errors (or faults) to multiple event correlation and complex analysis. It is designed to send a notification only when an event or series of events has occurred that requires a service action.

A Service Tools CD is included with the HP Command View EVA package. However, it is always best to check the HP web site for the latest updates.

The latest WEBES kit can be downloaded from this URL: http://h18000.www1.hp.com/support/svctools

EVA remote support tools

As a no-charge option, HP will install ISEE remote service tool for any Enterprise Virtual Array under warranty or service support. This tool enables EVA self-monitoring and diagnosis. ISEE can significantly reduce the time required to isolate and correct problems. If desired, the tool can be configured to transmit status information directly to an HP service center for proactive problem resolution. Contact your local HP Services department for details.

Customer Self Repair (CSR) support

To benefit those customers who prefer the convenience of replacing failed components themselves, the EVA4000/6000/8000 and WEBES (described above) have been designed to facilitate customer self repair. For more information, see the Hewlett-Packard Company Limited Warranty at http://h18006.www1.hp.com/products/storageworks/warranty.html, the EVA4000/6000/8000 User Guide, or contact HP Services.

The following hardware components are customer replaceable:

- Disk drives
- Controller blowers
- Controller power supplies
- Controller cache batteries
- Disk enclosure power supply/blowers

EVA 4000/6000/8000 overview

Software

Table 2 lists the HSV controller software and the optional software products supported on the EVA 4000/6000/8000.

Table 2 HP StorageWorks Enterprise Virtual Array 4000/6000/8000 software

Software	Version	Description
HP StorageWorks Virtual Controller Software v3.0d media kit for dual HSV210 and 200 controllers	5.020	Required for EVA4000, EVA6000, and EVA8000
HP OpenView Storage Management Appliance software	2.1	Required with XCS 5.020 system software.
HP StorageWorks Command View EVA	4.0	Required with XCS 5.020 system software.
HP StorageWorks Business Copy EVA	3.0	Optional. Offers enhanced management capability of local replication.
HP StorageWorks Continuous Access EVA	2.1	Optional. Offers enhanced management capability of remote replication.
Replication Solutions Manager (RSM)	1.1	Optional. A new HP interface that offers enhanced management capability of both local and remote replication. RSM 1.1 comes with HP Continuous Access 2.1 and HP Business Copy 3.0.

XCS Media Kit for Dual HSV controllers

The following items are included in the XCS Media Kit for Dual HSV210/200 Controllers.

- XCS Upgrade License
- HP StorageWorks System Software for HSV210/200 5.020 CD-ROM
- HP StorageWorks 4000/6000/8000 Enterprise Virtual Array Documentation CD-ROM

HP StorageWorks Command View 4.0 is required for XCS 5.020 and can be purchased separately.

Licensing information

The following optional licenses are available for XCS 5.020:

- HP Business Copy EVA license to use (LTU) activates the local replication (snapshot and snapclone) functionality and is licensed by capacity. For detailed licensing and ordering information, refer to the *HP StorageWorks Business Copy EVA quickspecs* at the following web site:
  http://h18006.www1.hp.com/products/storage/software/bizcopyeva/specifications.html
- HP Continuous Access EVA license to use (LTU) activates the remote replication functionality and is licensed by capacity. For detailed licensing and ordering information, refer to the *HP StorageWorks Continuous Access EVA quickspecs* at the following web site:
  http://h18006.www1.hp.com/products/storage/software/conaccesseva/specifications.html

For assistance with an incorrect Authorization ID, contact an HP-authorized service provider. For assistance with a lost Authorization ID or missing Authorization ID, contact your HP order channel.

Supported components

This section identifies the hardware and software components supported by the EVA 4000/6000/8000.

Supported system configurations

For complete information on supported configurations, refer to the *HP StorageWorks 4000/6000/8000 Enterprise Virtual Array QuickSpecs*, which can be downloaded from appropriate web site:

http://www.hp.com/go/eva4000

http://www.hp.com/go/eva6000

http://www.hp.com/go/eva8000

Supported operating system specifications

Detailed system specifications for each supported operating system are included in a series of *Connectivity Installation and Reference Guides* and associated *Connectivity Release Notes*. You can download the information necessary for your operating environment at the appropriate web site:

http://www.hp.com/go/eva4000

http://www.hp.com/go/eva6000

http://www.hp.com/go/eva8000

Click the **Technical documentation** link under Product information.

Supported disks

Table 3 lists the supported Fibre Channel disks.

NOTE:

- A minimum of eight disks is required to create a disk group. Additional disks may be added up to the established disk group limits.
- A disk group cannot contain both online (high performance) disks and FATA disks. It must contain only one type of disks.

Table 3 Supported disks

Fibre Channel disk	HP model displayed in HP Command View EVA	Minimum firmware revision
High-performance disks		
10K RPM 36-GB	BD03654499	3BE9
	BD03655B28	HP00
	BD03656ABA	HP09
	BD03659532	HP01
10K RPM 72-GB	BD07254498	3BE9
	BD07254498	3BE9
	BD07255B29	HP00
	BD07256ABB	HP09
	BD07258224	HP01
	BD0725822B	HP01
10K RPM 146-GB	BD14656ABC	HP09
	BD14658225	HP01
	BD14655B2A	HP00
	BD1465822C	HP01
10K RPM 300-GB	BD30058226	HP00
	BD30058232	HP00
15K RPM 36-GB	BF03654564	3BE9
	BF03655B2B	HP00
	BF03658242	HP00
	BF036574C9	HP05
15K RPM 72-GB	BF07255B2C	HP00
	BF0725754B	HP00
	BF07258243	HP00
15K RPM 146–GB	BF14658244	HP00
FATA (near-online) disks		
250-GB	ND2505823A	HP00
	ND25058238	HP00

Operating constraints

This section identifies operating constraints specific to the EVA 4000/6000/8000 hardware and XCS software. Operating constraints for related software applications are included in the following documents:

- *HP OpenView Storage Management Appliance Software release notes*
- *HP StorageWorks Command View EVA 4.0 release notes*
- *HP StorageWorks Continuous Access EVA 2.1 release notes*
- *HP StorageWorks Business Copy EVA 3.0 release notes*
- *HP StorageWorks Replication Solution Manager 1.1 release notes*

Any operating constraints pertaining to the host operating system can be found in the individual operating system release notes.

Windows 2003 MSCS Cluster installation

The MSCS cluster installation wizard on Windows 2003 may fail to find the shared quorum device and disk resources may not be auto created by the cluster setup wizard. This is a known Windows Cluster Setup issue that has existed since Win2003 RTM.

There are two possible workarounds for this problem:

- The issue and recommended workaround are described in the following Microsoft support article: *Shared disks are missing or are marked as "Failed" when you create a server cluster in Windows Server 2003* (ID 886807), which can be downloaded from the following web site:
  http://support.microsoft.com/default.aspx?scid=KB;EN-US;886807
- This issue can also be bypassed by setting the load balancing policy for each LUN to NLB using the MPIO DSM CLI.

Microsoft is currently working on a resolution to address this issue.

Host port connection limit on B–series 3200/3800/3850 switches

The EVA 4000/6000/8000 is limited to a maximum of three host ports on a single 8- or 16-port B-series 3200/3800/3850 switch. This limit *does not* apply to a B-series 3850 switch running V4.4.0C or later firmware, or to other supported B-series, C-series or M-series switches.

Connecting more than three ports to a single switch may result in dropped connections between the array and the host. Connections are typically dropped following an array controller resynchronization, or when an event impacts the fabric, such as rebooting or adding a switch.

The following options can be used to avoid or manage the port limitation:

- Distribute the array host port connection across multiple switches to ensure that no more than three host ports are connected to a single switch. This is the recommended option for avoiding dropped connections and maintaining availability.
- Reduce the number of array host port connections to the fabric. This option is useful if you have a limited number of switches, however it will impact availability by reducing the number of paths to the array.
- Connect more than three array host ports to a switch, with the understanding that connections may be dropped. Connections that are dropped can usually be reestablished as follows:

  1. Use the Brocade `switchshow` command to identify which ports have failed.
  2. Disconnect the Fibre Channel cable from the failed port.
  3. Wait 10 seconds and reconnect the cable. This will cause the port to re-log into the fabric and reestablish connection to the array.

Direct Connect Configuration Requirements

When using direct connect configuration on Windows, make sure the following requirements are met:

- When using Emulex or Qlogic HBAs, set the HBA topology parameter to 0 (Loop only). The default value is 2 (Loop then F-Port). Using the default value may increase the amount of time required for the host to connect to the storage system.
- The HSV200/210 controller firmware cannot differentiate between an empty host port and a failed host port in a direct connect configuration. As a result, the Connection state dialog box on the Controller Properties window displays *Connection failed for an empty host port*. To fix this problem, insert an optical loop-back connector into the empty host port; the Connection state will display *Connected*. For more information about optical loop-back connectors, contact your HP-authorized service provider.

Restoring I/O paths on Windows following a controller failure

When operating on Windows, some I/O paths to a failed controller may not be restored when the controller is returned to normal operation. In this situation, it will be necessary to disable and re-enable the appropriate switch ports to restore the I/O path.

NOTE:

If this situation occurs, contact HP Support immediately for assistance in resolving the problem. This issue will be resolved in a future XCS release.

Configuring your system for notification of failed I/O paths

To ensure you are notified immediately if this situation occurs, your system should be configured to alert you when failed I/O paths are detected. This includes configuring HP MPIO DSM Manager to provide email notification.

Configuring HP MPIO DSM Manager email notification utility

1. Open the HP MPIO DSM Manager Notification Editor by clicking on **Start** > **Programs** > **Hewlett-Packard** > **MPIO DSM Manager** > **Configure Notification Utility**

   For help on configuring the notification utility, click **Help** at any time.
2. Select **Enable Email Notification Events**
3. Enter the name or the IP address of the SMTP server which will handle email delivery in the **SMTP Server Domain Name or IP Address** field.
4. Enter the TCP server port number in the **SMTP Server Port** field. If you wish to listen on the default SMTP port (25), this field can be left unchanged.
5. Select **SMTP Authentication** to authenticate the sender of the email.

   If SMTP Authentication is selected, enter the login name and password information in the respective fields. If the SMTP server accepts anonymous logins, these fields may be left blank.
6. Enter the destination email address for notifications in the **Send "To" Address** field. To send notifications to multiple recipients, enter each email address separated by a semicolon (;).
7. Enter the sender email address for notifications in the **Use "From" Address** field.
8. Enter the Reply To email address in the **Use "Reply To" Addr** field. To use the From address as the Reply To address, leave this field blank.
9. Click **Send Test Email** to send a test email and validate the selected settings.
10. Click **OK** to save the settings and exit the editor.

Restoring I/O paths

If any I/O paths are lost following a controller failure, use the following procedure to restore them.

NOTE:

Perform the following steps for each failed I/O path. Paths must be restored on one HBA at a time.

1. Identify an HBA that is part of a failed I/O path.
2. Identify the switch port the HBA is connected to.
3. Disable and re-enable the associated switch port using the appropriate procedure in Disabling/enabling switch ports.

NOTE:

Make sure you wait the required 60 seconds after disabling the port before re-enabling it.

4. Use HPDSM or MPIO GUI to verify that the failed path has been restored.

Disabling/enabling switch ports

The following procedures describe how to disable and enable a switch port on each of the supported FC switches.

B-series switches

B-series switch ports can be disabled or enabled using either the CLI or GUI. You may find it easier to use CLI/telnet commands.

Using the CLI

1. Login to the switch with admin access.
   a. Telnet to the switch using the switch symbolic name or the IP address.
   b. Login as admin and provide the password when prompted. The default switch password is "password".
2. Identify the switch port to be disabled and enter `portDisable port#`
3. Wait 60 seconds and continue with the next step.
4. Enter `portEnable port#`

Example of disabling/enabling switch port 8:

```
telnet 15.43.214.186
Fabric OS (BR39_01)
BR39_01 login:  admin
Password:
BR39_01:admin> portDisable 8
```

Wait 60 seconds and then enable the port

```
BR39_01:admin> portEnable 8
BR39_01:admin>
```

Using the GUI

Launch Web Tools or the GUI by entering the IP address of the switch in a web browser connected to the network. When the switch graphic is displayed, perform the following steps.

1. Click on the **Admin** tab to access the switch Administration Window.
2. Enter the admin user name and password.

3. Select the **Port Setting** tab.
4. Identify the number of the switch port that needs to be disabled and clear the **Enable Port** check box for that port.
5. Click **Apply**, and click **Yes** when prompted.
6. Wait 60 seconds and continue with the next step.
7. Select the **Enable Port** check box to re-enable the port.
8. Click **Apply**, and click **Yes** when prompted.
9. Check the log at the bottom of the screen for information regarding the switch configuration changes.

Cisco C-series switches

Cisco switch ports can be disabled or enabled using either the management console, telnet, or Device Manager.

Using the management console or telnet

NOTE:

Your login account must have network-admin privileges to perform this procedure.

1. Log into the switch using either the management console or by telnet.
2. Log in to your network-admin privileged account using your login name and password.
   Verify the line card number and port number of the port to be disabled and re-enabled.
3. Enter the following, substituting the appropriate fc numbers. In this example, fc 1/5 represents line card 1, port 5:

```
switch# config terminal
switch(config)# interface fc 1/5
switch(config-if)# shutdown
```

   Wait 60 seconds and continue with the next command to enable the port.

```
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# exit
```

Using Device Manager

NOTE:

Your login account must have network-admin privileges to perform this procedure.

1. Open Device Manager.
2. Log in to your network-admin privileged account using your login name and password.
3. Right-click on the appropriate port and select **Disable**
4. Click **Yes** when asked to confirm port disabling.
5. Wait 60 seconds and continue with the next step.
6. Right-click on the same port and select **Enable**

McData M-series switches

On M-Series products, ports can be disabled and enabled by performing a port block and unblock operation. This is done by accessing switch management using the ha-Fabric Manager, the Embedded

Web Server GUI resident in the director or edge switch, or using the Command Line Interface to the director or edge switch.

Using ha-Fabric Manager (HAFM)

1. Login to HAFM application.
2. Open the Element Manager for the director or edge switch whose port is to be blocked. To open the Element Manager, perform one of the following steps:
   - Right-click a director or edge switch icon and select **Element Manager**
   - Double-click a director or edge switch icon.
3. Block and unblock the desired port. Port operation is controlled using the Configure Ports dialog box in the Element Manager window:
   a. Click **Configure > Ports**. The Configure Ports dialog box is displayed.
   b. Block operation for the desired port(s) by selecting the check box in the Blocked column. When selected, the port will be blocked when the change is activated.
   c. Click **Activate** to invoke the changes and close the dialog box.
   d. Wait 60 seconds before continuing with the next step.
   e. Unblock operation for the desired port(s) by clearing the check box in the Blocked column. When cleared, the port will be unblocked when the change is activated.
   f. Click **Activate** to invoke the changes and close the dialog box.

Using the Embedded Web Server

1. Login to the Embedded Web Server for the director or edge switch whose port is to be blocked. The director or edge switch View is displayed.
2. Click on **Configure** in the navigation panel. The Configure page and the Ports tab view displays.
3. Select the check box in the Blocked column to block a port (default is unblocked). A check mark indicates the port is blocked.
4. Click **Activate** to save and activate the changes. The following message is displayed: "Your changes to the port configuration have been successfully activated".

NOTE:

Because the Director 2/140 has many ports, the listing of ports is divided into separate displays, which are accessed by clicking the hyperlinks 1-31, 32-63, 64-95, 96-127, and 132-143. (Ports 128 through 131 are internal ports and not available for external connections.) If you make any changes to a particular list of ports, click **Activate** before selecting another list of ports. If you do not click **Activate**, changes are not implemented on the director.

5. Click on the **Ports** tab to return to the Ports tab view if more changes are desired.
6. Wait 60 seconds before continuing with the next step.
7. Clear the check box in the Blocked column to unblock the port. A check mark indicates the port is blocked, no check mark indicates the port is unblocked.
8. Click **Activate** to save and activate the changes. The following message is displayed: "Your changes to the port configuration have been successfully activated".
9. Click on the **Ports** tab to return to the Ports tab view if more changes are desired.

Using the CLI

The syntax for the command to block and unblock ports is:

```
config port blocked <portNumber> <blockedState>
```

This command has two required parameters.

`<portNumber>` specifies the port number. Valid values are:

0–11 for the Edge Switch 2/12

0–15 for the Edge Switch 2/16

0–23 for the Edge Switch 2/24

0–31 for the Edge Switch 2/32

0–63 for the Director 2/64

0–127 and 132–143 for the Director 2/140

`<blockedState>` Specifies the blocked state for the port. Valid values are true and false. Boolean 1 and 0 may be substituted as values. Value true or 1 blocks the port; value false or 0 unblocks the port.

To use CLI to block and unblock a port, perform the following procedure:

1. Login to the Command Line Interface for the director or edge switch whose port is to be blocked. The prompt `Root>` is displayed.
2. To block a port, enter the following command:
   ```
   Root> config port blocked <portNumber> true
   ```
3. Wait 60 seconds before continuing with the next step.
4. To unblock the port, enter the following command:
   ```
   Root> config port blocked <portNumber> false
   ```
5. Repeat steps 2 through 5 for additional ports.
6. Enter the following command:
   ```
   Root> logout
   ```

Avoiding problem situations

NOTE:

Refer to Chapter 3, "Operation" of the *HP StorageWorks 4000/6000/8000 Enterprise Virtual Array user guide* for additional hints and helpful information.

Information on avoiding problem situations specific to operating systems can be found in the individual operating system release notes.

Disk Resource Pending Timeout for Microsoft® Windows® Cluster configurations

If the disk resource count is greater than 8, HP recommends increasing the Pending Timeout parameter for each disk resource from 180 seconds to 360 seconds. Increasing the timeout value helps maintain continuous operation of disk resources across SAN perturbations.

To view and set the Pending Timeout parameter:

1. Open the Microsoft Cluster Administrator.
2. Select a Disk Group resource in the left pane.
3. Right click Each Disk Resource in right pane, one at a time, and select Properties.
4. Select the Advanced tab from the Properties menu.
5. Locate the Pending Timeout value and change it to 360.
6. Click OK.

Documentation updates

No updates at this time.